Technical infrastructure and security

Panopto cloud video platform

Panopto

Contents

Introduction

Panopto's online video platform can be deployed either as a cloud-hosted service or as an on-premises solution. With the cloud-hosted service, Panopto maintains server infrastructure and ensures its continuous, optimal delivery.

This document covers the physical infrastructure and security protocols of the Panopto cloud-hosted service. It provides specifications for all of the hardware components, network routing, and application security features that comprise the Panopto Cloud. Information detailing network security for Amazon Web Services (AWS) – which provides the backbone for the Panopto Cloud – as well as information on backup procedures, redundancy, and protection against common security threats is included.

Architecture

Hardware and software

Panopto's cloud service enables customers to use Panopto software hosted on Panopto servers.

Panopto Cloud is hosted on Amazon Web Services with geographic server options in the United States, European Union, Canada, and Asia Pacific.

Panopto Cloud is secure, scalable, has high availability for redundancy, and is built to ensure uptime and reliability.

The Panopto software is installed on Amazon EC2 instances, uses Amazon S3 for content storage and Amazon CloudFront as the content delivery network.

Panopto cloud components

Web server components

- Microsoft Windows Server 2019
- Internet Information Services (IIS) 10.0
- Microsoft .Net Framework 4.6.2

Data server components

- Microsoft Windows Server 2019
- Microsoft .Net Framework v 4.6.2
- Microsoft PowerPoint 2016

Database server components

- Microsoft Windows Server 2019
- Microsoft SQL Server 2019 – latest update

Amazon server locations

Amazon EC2 is hosted in multiple locations worldwide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. Amazon EC2 provides the ability to place instances and data in multiple locations. Panopto's cloud operates out of multiple US East (us-east-1), EU West (eu-west-1), AP Southeast (ap-southeast-1), and CA Central (ca-central-1) availability zones, located in the US, Ireland, Singapore, and Montreal.

Amazon content backup and disaster recovery

All of the content for Panopto Cloud is stored in Amazon S3, which is designed to provide 99.999999999% durability of objects over a given year. Data is redundantly stored across multiple Availability Zones using multiple devices in each facility. Each Availability Zone runs on its own physically distinct, independent infrastructure and is engineered to be highly reliable. Common points of failure like generators and cooling equipment are not shared across Availability Zones. Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone.

Panopto database and security log backup

For disaster recovery and security purposes, Panopto stores copies of its SQL database backups and security log information in geographically and logically fully distinct regions.

SQL database and security log backup locations:

NA Cloud: US East (Ohio) Region

EU Cloud: Europe (London) Region

AP Cloud: Asia Pacific (Sydney) Region

CA Cloud: Europe (Ireland) Region

This backup process increases metadata durability in the event of a catastrophic AWS region failure, improves protection against data integrity failures, and provides tamper resistance from malicious actors.

All data is encrypted at rest and in transit. Please refer to "Encryption" below for more information on Panopto's encryption standards.

Panopto will retain this data for up to five (5) years.

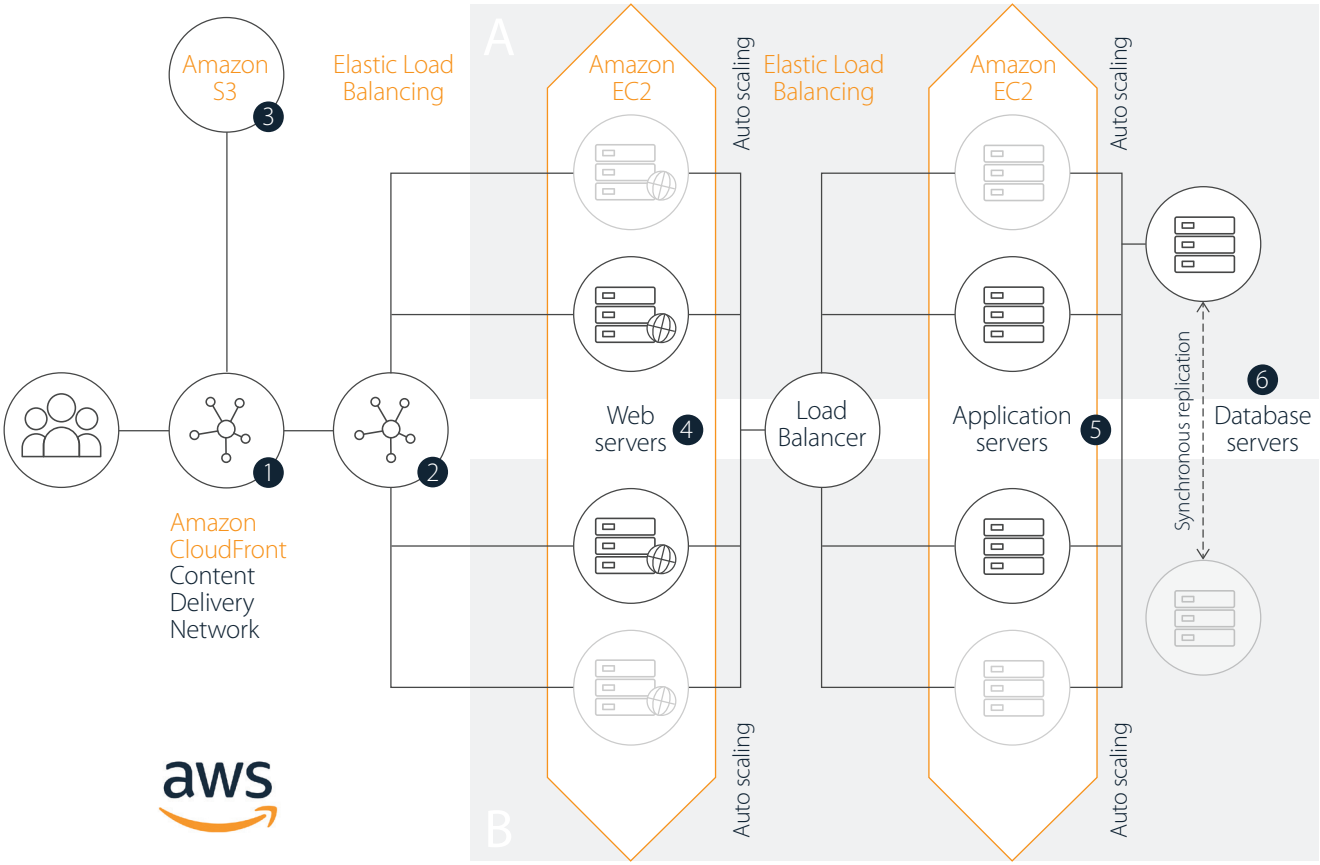
Panopto server redundancy and business continuity

The Panopto Cloud solution offers redundancy in multiple Amazon Availability Zones, eliminating single points of failure and providing additional reliability. This design provides redundancy for servers used in the hosted architecture including; web servers, data servers, and the database server.

Panopto's relational database is mirrored between multiple Availability Zones within the region.
In the event that a single server goes offline, other servers will still be available for use. In the event of an availability zone going completely offline, the architecture allows the other availability zone to still be available for use. This ensures that customers are not affected by an availability zone outage.

Panopto

Example diagram of Panopto's cloud architecture



Architecture overview

1. The Amazon CloudFront CDN is a global network of edge locations and regional edge caches that temporarily stores content close to viewers. Amazon CloudFront ensures that end-user requests are served by the closest edge location, enabling viewer requests to travel a shorter distance. This improves performance.

2. HTTPS requests are handled by Elastic Load Balancing which automatically distributes incoming application traffic across multiple Panopto Web Servers across multiple Availability Zones (AZs). This enables greater fault tolerance, and seamlessly provides load balancing capacity needed in response to incoming user traffic.

3. Resources and static content used by Panopto Web Servers are stored in Amazon Simple Storage Service (S3), a highly durable storage infrastructure designed for mission-critical and primary data storage. S3 is available across all Availability Zones.

4. Panopto uses multiple Web Servers in multiple Availability Zones, providing reliability and redundancy for customers. Auto Scaling provides Panopto with the on-demand ability to increase the number of Web Servers to accommodate increased traffic.

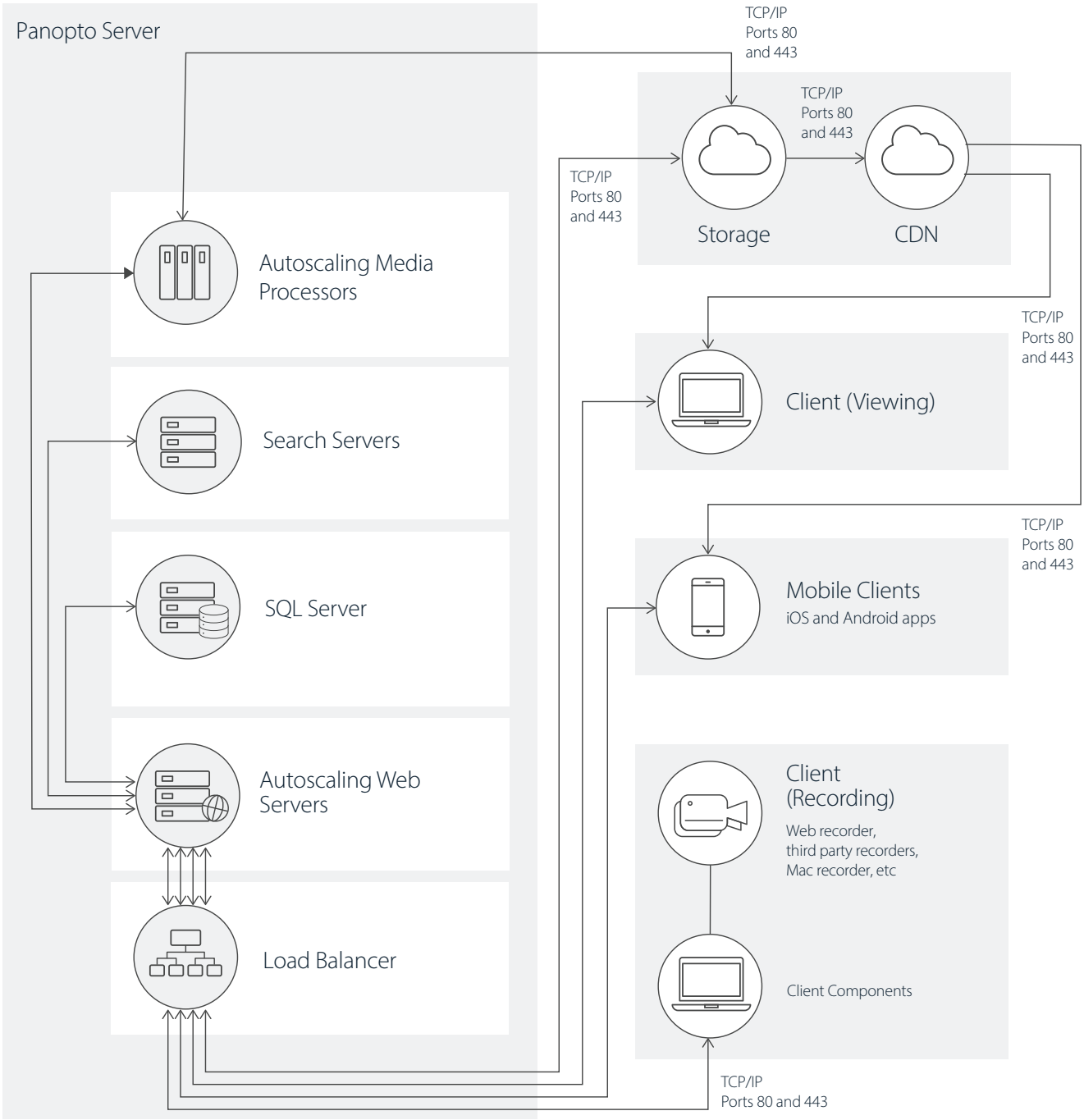
5. Multiple Application Servers or Data Servers are used in multiple Availability Zones, providing reliability and redundancy to ensure that all content is encoded quickly for customers. Additional Data Servers can be added to accommodate increased encoding needs from customer uploads.

6. Panopto's SQL databases are located in multiple Availability Zones and feature synchronous high-safety database mirroring with automatic failover, providing reliability and fault tolerance.

Panopto server architecture

The following diagram displays the Panopto server architecture of a single availability zone, the components of each server, and the interaction with the client.

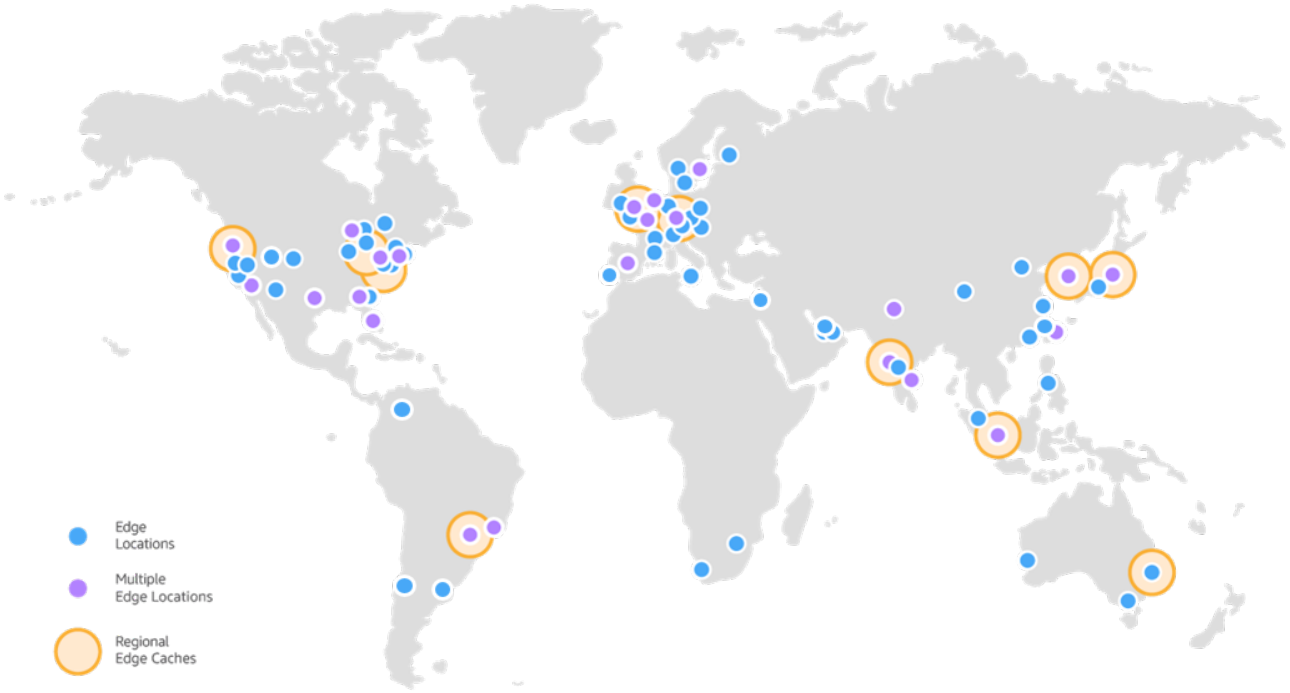
(Note: The amount of servers being used is for reference only; servers are added as needed to accommodate usage).



Panopto content delivery with Amazon CloudFront

Amazon CloudFront employs a global network of edge locations and regional edge caches that cache copies of content close to viewers. Amazon CloudFront ensures that end-user requests are served by the closest edge location. As a result, viewer requests travel a short distance, improving performance for viewers. For files not cached at the edge locations and the regional edge caches, Amazon CloudFront keeps persistent connections with Panopto's origin servers so that those files can be fetched from the origin servers as quickly as possible.

To deliver content to end users with lower latency, Amazon CloudFront uses a global network of 210 Points of Presence (199 Edge Locations and 11 Regional Edge Caches)* in 78 cities across 37 countries.



* Panopto does not make use of any mainland Chinese CDNs.

Amazon continously adds new CDN PoP locations.

For more information and an up-to-date list of edge locations, visit: https://aws.amazon.com/cloudfront/details

Security

Amazon EC2 security

Certifications, accreditations, frameworks

AWS is compliant with various certifications and third-party attestations. These include:

Certifications / attestations

- CS [Germany]
- Cyber Essentials Plus [UK]
- DoD SRG
- FedRAMP
- FIPS
- IRAP [Australia]
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MTCS [Singapore]
- PCI DSS Level 1
- SEC Rule 17-a-4(f)
- SOC 1
- SOC 2
- SOC 3

Laws, regulations, and privacy

- CISPE
- EU Model Clauses
- FERPA
- GLBA
- HIPAA
- HITECH
- IRS 1075
- ITAR
- My Number Act [Japan]
- U.K. DPA - 1988
- VPAT/Section 508
- EU Data Protection Directive
- Privacy Act [Australia]
- Privacy Act [New Zealand]
- PDPA - 2010 [Malaysia]
- PDPA -2012 [Singapore]
- PIPEDA [Canada]
- Spanish DPA Authorization

Alignments / frameworks

- CIS
- CJIS
- CSA
- ENS [Spain]
- EU-US Privacy Shield
- FFIEC
- FISC
- FISMA
- G-Cloud [UK]
- GxP [FDR 21 Part 11)
- ICREA
- IT-Grundschutz [Germany]
- MITA 3.0
- MPAA
- NIST
- PHR
- Uptime Institute Tiers
- UK Cloud Security Principles

For more information on risk and compliance activities in the AWS cloud, consult the Amazon Web Services Risk and Compliance whitepaper which can be found at: https://d1.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

Network security

The AWS network provides significant protection against traditional network security issues, and Panopto's Cloud Operations Team has implemented additional measures for further protection. The following are a few examples:

Distributed Denial of Service (DDoS) attacks

AWS Application Programming Interface (API) endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

Man In the Middle (MITM) attacks

All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and logs them to the instance's console.

IP spoofing

Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port scanning

Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated.

Encryption

All user data being uploaded to Panopto or viewed by end-users is protected in transit to and from the Panopto system through the use of TLS v1.2 encryption. For the protection of data at rest, Panopto utilizes Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). Each object in Panopto's S3 bucket is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt data.
For more information about SSE-S3: https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

Environmental safeguards

Physical access

AWS data centers are state of the art, utilizing innovative architectural and engineering approaches. AWS has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire detection and suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

AWS monitors electrical, mechanical and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage device decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses techniques detailed NIST 800-88 ("Guidelines for Media Sanitization as part of the decommissioning process").

Components

The Panopto components listed in this document also have multiple levels of security. You can view a whitepaper for each component at the links listed below.

Panopto components

Microsoft Windows Server 2019
https://www.microsoft.com/en-gb/cloud-platform/windows-server

Microsoft SQL Server 2019 SP1 CU2
https://www.microsoft.com/en-us/sql-server/sql-server-2019

HTTP Live Streaming
https://developer.apple.com/streaming

IIS 10.0
http://learn.iis.net/page.aspx/110/changes-in-security-between-iis-60-and-iis-7-and-above

.Net 4.6.2 Framework
https://www.microsoft.com/en-us/download/details.aspx?id=53344

Panopto application security

API and integrations

Our API is publicly available and can be configured for use with other platforms. Panopto currently provides integrations for various platforms.

Auditing

Panopto software tracks a variety of data such as which user creates or deletes a session.

Client-side and Server-side validation

The user authenticates on the Panopto client application. The client encrypts the password and sends it to the server. The server checks the password with the hashed password.

Encryption of user information

Panopto uses SSL in the web interface to encrypt all sensitive user information. The Panopto server uses password hash checking. Passwords are not stored as plaintext.

Inbound data validation

The Panopto software checks and tests for valid data as well as protects against SQL injection and other malicious inputs. Validation of all data is handled on the client-side where possible, but the server never responds with sensitive validation data.

Passwords and authentication

Panopto secures the video repository perimeter with support for multiple credential types, including OAuth, SAML 2.0, Active Directory, and a number of LMS ID providers.

Panopto's single-sign on (SSO) implementation supports rolling two-way synchronization of credentials, ensuring that user information is always up to date.

Additionally administrators have the ability to enforce strong passwords, set password expiration, require two-factor authentication via SSO and define session timeout.

Role based access

Roles are specifically assigned to each user account (Administrator, Videographer, Creator, and Viewer).

Software development

The Panopto development team has a formal SDLC that is followed for each release. Because Panopto is a private company, we are not able to disclose the details of our development lifecycle.

Session time out

The web interface has a configurable session time out in place. The time out is based on the expiration of the cookie. The cookie is valid for 2 weeks after first log in.

User access control

Panopto allows for content to have two access levels; "Public" and "Unlisted". Public content can be accessed by anyone that has the URL or the ability to browse to the session. Unlisted content requires the user to specifically be given access to the content. All unlisted content requires the user to be logged in to view the content.

Availability and maintenance

Panopto SLA

For purchasers of our hosted solution, Panopto will continue, for the Term of the Agreement, to offer hosting services to the Licensee. Panopto will use reasonable efforts to make the hosting services available 7 days a week, 24 hours a day. Panopto shall make the hosting services available, as measured in accordance with the formula below over the course of any one-month period, an average of 99.9% of the time. "Available" means that the end user or intersystem action requests receive a response within thirty (30) seconds. "Unavailable" means that the hosting services are not available. "Hosting Availability" is expressed generally as a percentage of the requested hours during which the hosting services are available for use by Licensee.

Amazon SLA

Amazon Web Services will use commercially reasonable efforts to make Amazon EC2 available with an Annual Uptime Percentage (defined in Appendix A) of at least 99.95% during the ServiceYear.

Planned Uptime is the total number of hours (TH) in each calendar month. Hosting Availability is calculated as follows and is measured on a calendar month basis

$$HA = \frac{100 \times (1 - (DH - SDH))}{TH}$$

HA	Hosting Availability
DH	Total of all downtimes measured in hours
SDH	Total of all agreed and scheduled downtimes, not to exceed three (3) hours in any month, measured in hours
TH	Total hours in each calendar month

Upgrades and maintenance

The Panopto Cloud servers are upgraded to the latest version of the Panopto software when it is released. Typically there are two major upgrades per year. All expected downtime will be planned for non-core hours, on a weekend, varying by cloud location. Typical downtime windows start after 6pm local time and end before 8am local time, for primary locations served by the cloud.

During the time your site is offline, you will not be able to access recordings on your server, and any attempts to upload from clients will result in a "Server unable to connect" message. Scheduled recordings will capture offline and upload after the site is back online.

Recorder clients are able to select the record offline option and upload after the site is back online.

The duration of the downtime window can vary from release to release, but it typically ranges from two to four hours.

Customers are notified via email three weeks in advance of any planned downtime. Reminders will be sent via alert messages and will also be posted to trust.panopto.com.

Staging sites will be available prior to any major release.

Support will be available on live chat during upgrades and will be monitoring the ticket queue for widespread problems related to the upgrade (Authorized Point of Contacts only).

Support will not monitor live chat during planned maintenance or hotfixes.

Appendix A

Definitions

Annual uptime percentage is calculated by subtracting from 100% the percentage of 5 minute periods during the Service Year in which Amazon EC2 was in the state of region unavailable.

AWS means Amazon Web Services.

Cloud solution means the licensed products, subject to the purchase of usage bundles described below, that are made available to the licensee by means of the internet or other electronic means, which are installed and maintained by Panopto on Panopto controlled servers and that Panopto provides access to and support for the licensed products for authorized uses as further described in the Panopto Software License and Services Agreement. Access shall be accomplished through a password protected site. Panopto shall create and maintain, on its server, a management page for each licensee, which page shall show then-current usage statistics for such licensee. Components of the hosted solution may be delivered to the hosted solution for installation on the licensee's equipment for use with the hosted solution.

Panopto means Panopto,Inc.,a Delaware corporation,including its successors and assigns.

Panopto recorder software/Panopto client means all of the software owned by Panopto and licensed to the licensee hereunder that is installed on computers located at the primary location for purposes of enabling the production of content.

Panopto software means the Panopto recorder software and the Panopto server software.

Update means either (i) a modification or addition that, when made or added to the licensed products, establishes material conformity of the licensed products to the functional specifications, or (ii) a procedure or routine that, when observed in the regular operation of the licensed products, eliminates the practical adverse effect on the licensee of such nonconformity. Updates are designated by a change in the number to the right of the second decimal point (V.X.1).

Upgrade means any modification or addition that materially changes the software's utility, efficiency, functional capability, or application but is not separately priced and marketed by Panopto and does not constitute an Update. Panopto may designate upgrades as minor or major, depending on Panopto's assessment of their value and of the function added to the preexisting licensed products. Such determination shall be at the sole discretion of Panopto. Upgrades are designated by a change in the number to the right of the first decimal point (V.1.Y) language.